Exhibit 2

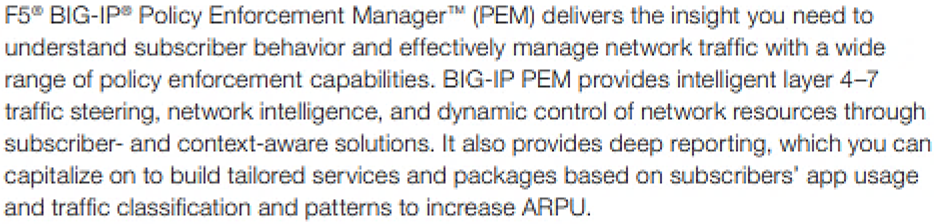
US8248940B2	Specification Support	F5 Networks BIG-IP Policy Enforcement Manager (PEM) (The accused product)
15Pre. A method of targeted content delivery in a packet-based communication network in communication with a terminal device based on Internet video traffic analysis, comprising:	FIG. 1 is a schematic diagram of a first exemplary embodiment of **a system 100 for targeted content delivery based on Internet video traffic analysis.** Exemplary **system 100 depicts the basic communication framework between an Internet user and a content provider.** [Col. 3, Line 51-55]	The accused product performs a method of targeted content delivery in a packet-based communication network in communication with a terminal device based on Internet video traffic analysis, comprising: F5 Networks provides BIG-IP products. F5's BIG-IP is a family of products covering software and hardware designed around application availability, access control, and security solutions. F5 BIG-IP Policy Enforcement Manager (PEM) delivers the insight to understand subscriber behavior and effectively manage network traffic with a wide range of policy enforcement capabilities. BIG-IP PEM provides intelligent layer 4–7 traffic steering, network intelligence, and dynamic control of network resources through subscriber- and context-aware solutions. BIG-IP PEM provides deep reporting, which is used to build tailored services and packages (i.e. targeted content delivery) based on subscriber's app usage. See Fig. 1. **Citation 1: F5 BIG-IP PEM**  F5® BIG-IP® Policy Enforcement Manager™ (PEM) delivers the insight you need to understand subscriber behavior and effectively manage network traffic with a wide range of policy enforcement capabilities. BIG-IP PEM provides intelligent layer 4–7 traffic steering, network intelligence, and dynamic control of network resources through subscriber- and context-aware solutions. It also provides deep reporting, which you can capitalize on to build tailored services and packages based on subscribers' app usage and traffic classification and patterns to increase ARPU. **Fig. 1** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 1, last accessed May 14, 2020, Exhibit A

Exhibit 2

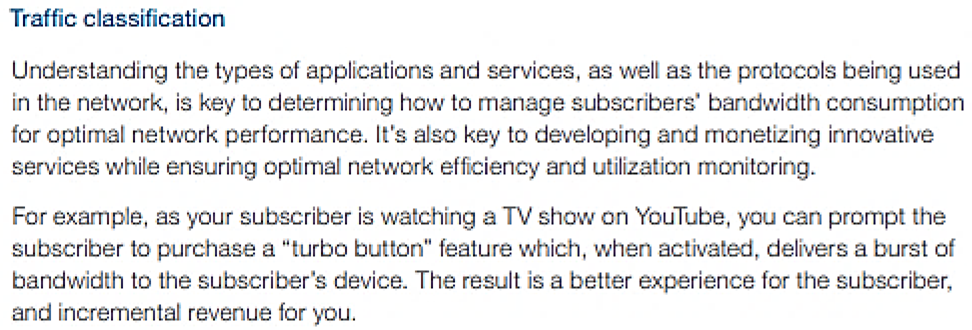
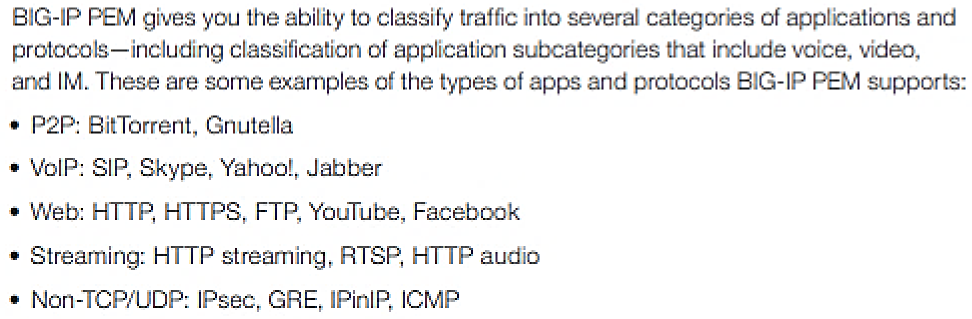
		BIG-IP PEM is used by service providers to deliver targeted content to the subscribers based on the analysis of videos viewed by a user. See Fig. 2. **Citation 2: Targeted content delivery**  Traffic classification Understanding the types of applications and services, as well as the protocols being used in the network, is key to determining how to manage subscribers' bandwidth consumption for optimal network performance. It's also key to developing and monetizing innovative services while ensuring optimal network efficiency and utilization monitoring. For example, as your subscriber is watching a TV show on YouTube, you can prompt the subscriber to purchase a "turbo button" feature which, when activated, delivers a burst of bandwidth to the subscriber's device. The result is a better experience for the subscriber, and incremental revenue for you. **Fig. 2** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, last accessed May 14, 2020, Exhibit A BIG-IP PEM classifies traffic into several categories of applications and protocols such as classification of application subcategories that include voice, video (i.e. internet video traffic analysis), and IM. See Fig. 3 **Citation 3: Traffic classification**

Exhibit 2



BIG-IP PEM gives you the ability to classify traffic into several categories of applications and protocols—including classification of application subcategories that include voice, video, and IM. These are some examples of the types of apps and protocols BIG-IP PEM supports:

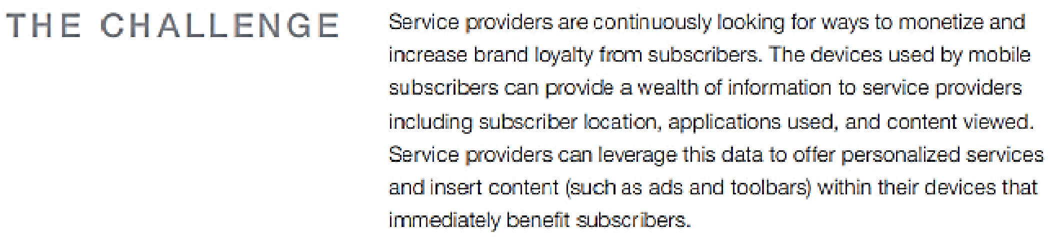
- P2P: BitTorrent, Gnutella
- VoIP: SIP, Skype, Yahoo!, Jabber
- Web: HTTP, HTTPS, FTP, YouTube, Facebook
- Streaming: HTTP streaming, RTSP, HTTP audio
- Non-TCP/UDP: IPsec, GRE, IPinIP, ICMP

Fig. 3

Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, last accessed May 14, 2020, Exhibit A

The BIG IP system including the BIG-IP PEM enables the service providers to insert content (i.e. targeted content delivery) to offer personalized services to benefit subscribers. The BIG-IP system including BIG-IP PEM helps in gaining subscriber and context awareness, and a deep understanding of subscribers' mobile preferences. See Fig. 4 & Fig. 5

Citation 4: Content Insertion



THE CHALLENGE

Service providers are continuously looking for ways to monetize and increase brand loyalty from subscribers. The devices used by mobile subscribers can provide a wealth of information to service providers including subscriber location, applications used, and content viewed. Service providers can leverage this data to offer personalized services and insert content (such as ads and toolbars) within their devices that immediately benefit subscribers.

Fig. 4

Source: https://f5.com/Portals/1/Premium/Architectures/GUIDE-SP-CCNF-66589956-customer-

Exhibit 2

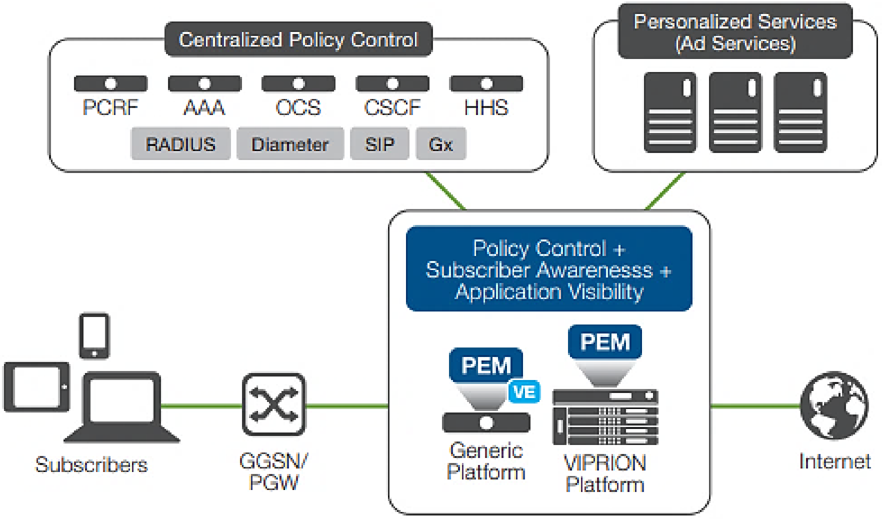
		usecase-2016-spreads.pdf, Page 17, Last accessed May 14, 2020, Exhibit B **Citation 5: Content Insertion**  Centralized Policy Control PCRF AAA OCS CSCF HHS RADIUS Diameter SIP Gx Personalized Services (Ad Services) Policy Control + Subscriber Awarenesss + Application Visibility PEM VE Generic Platform PEM VIPRION Platform Subscribers GGSN/ PGW Internet *Personalize the subscriber experience and increase revenue with content insertion.* **Fig. 5** Source: https://f5.com/Portals/1/Premium/Architectures/GUIDE-SP-CCNF-66589956-customer-usecase-2016-spreads.pdf, Page 17, Last accessed May 14, 2020, Exhibit B
15a. collecting, with a protocol signature identifier, relevant user traffic in the packet-based communication network;	the protocol signature identifier performs the **collecting** and comparing **traffic flows between the terminal device and one**	The method practiced by the accused product collects, with a protocol signature identifier, relevant user traffic in the packet-based communication network. BIG-IP PEM classifies traffic into several categories of applications and protocols such as classification into application subcategories which include voice, video, and IM. It can also

Exhibit 2

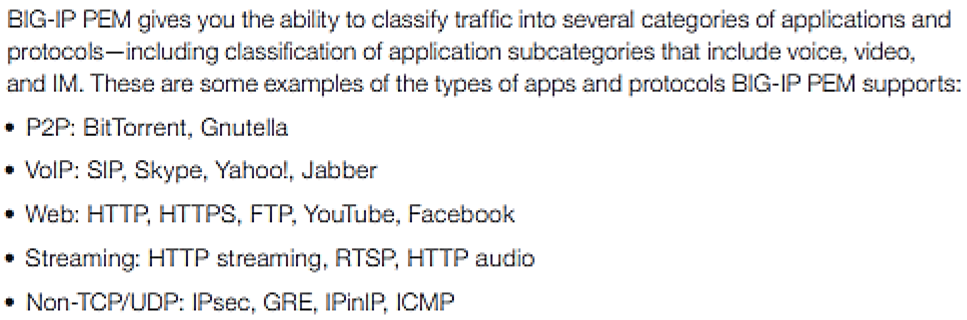
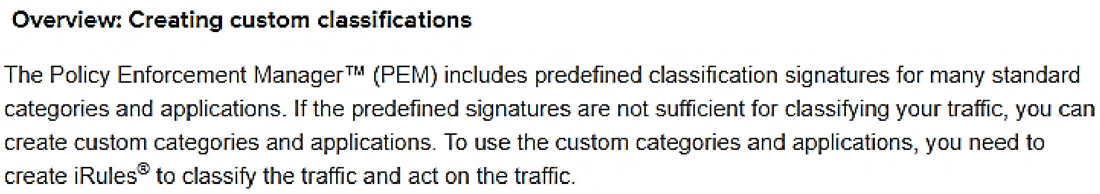
	or more video content sources to known protocol signatures, identifying one or more matches between the traffic flows and the known protocol signatures, and identifying, monitoring and analyzing the flow sequence of video content information for the identified one or more matches between the traffic flows and the known protocol signatures [Col. 2, Line 41-49]	classify the data as watching Youtube or HTTP streaming. See Fig. 6 **Citation 6: Traffic classification**  BIG-IP PEM gives you the ability to classify traffic into several categories of applications and protocols—including classification of application subcategories that include voice, video, and IM. These are some examples of the types of apps and protocols BIG-IP PEM supports: • P2P: BitTorrent, Gnutella • VoIP: SIP, Skype, Yahoo!, Jabber • Web: HTTP, HTTPS, FTP, YouTube, Facebook • Streaming: HTTP streaming, RTSP, HTTP audio • Non-TCP/UDP: IPsec, GRE, IPinIP, ICMP **Fig. 6** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, last accessed May 14, 2020, Exhibit A BIG-IP PEM includes predefined classification signatures for classifying traffic. Therefore, the BIG-IP PEM contains a protocol signature identifier to collect relevant user traffic in the communication network. If the predefined signatures are not sufficient, a user can also create custom categories and applications to classify the traffic. See Fig. 7 **Citation 7: Classification signatures**  **Overview: Creating custom classifications** The Policy Enforcement Manager™ (PEM) includes predefined classification signatures for many standard categories and applications. If the predefined signatures are not sufficient for classifying your traffic, you can create custom categories and applications. To use the custom categories and applications, you need to create iRules® to classify the traffic and act on the traffic. **Fig. 7**

Exhibit 2

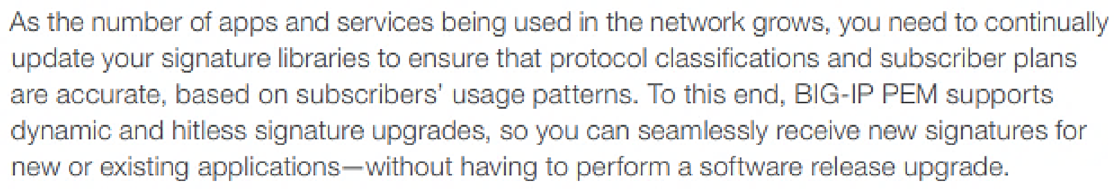
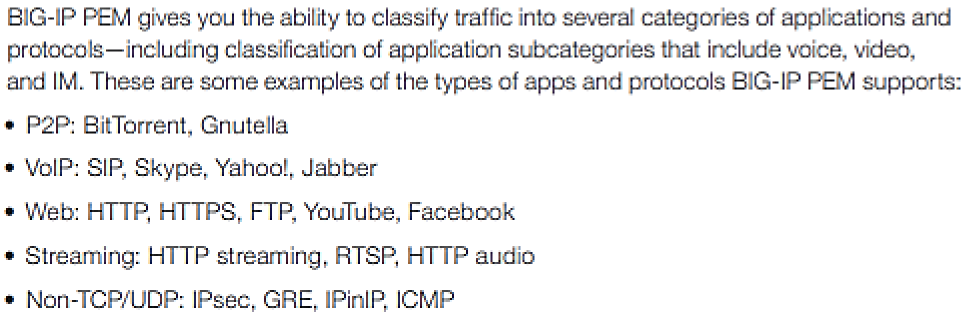
		Source: https://techdocs.f5.com/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-11-6-0/18.html, Page 1, Last accessed May 14, 2020, Exhibit C In BIG-IP PEM, signatures can be used for protocol classification. See Fig. 8 **Citation 8: Signature libraries**  As the number of apps and services being used in the network grows, you need to continually update your signature libraries to ensure that protocol classifications and subscriber plans are accurate, based on subscribers' usage patterns. To this end, BIG-IP PEM supports dynamic and hitless signature upgrades, so you can seamlessly receive new signatures for new or existing applications—without having to perform a software release upgrade. **Fig. 8** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, Last accessed May 14, 2020, Exhibit A
15b. comparing, with the protocol signature identifier, collected traffic flows of the relevant user traffic to a set of known protocol signatures;	In step 410, relevant user traffic is collected. The method 400 then proceeds to step 415. In step 415, collected traffic flows are **compared to a set of known protocol signatures**. Following step 415, the method 400 proceeds to step 420. [Col. 11, Line 48-50]	The method practiced by the accused product compares with the protocol signature identifier, collected traffic flows of the relevant user traffic to a set of known protocol signatures. BIG-IP PEM classifies traffic into several categories of applications and protocols such as classification intoo application subcategories that include voice, video, and IM. It can also classify the data as watching Youtube or HTTP streaming. See Fig. 9 **Citation 9: Traffic classification**

Exhibit 2



BIG-IP PEM gives you the ability to classify traffic into several categories of applications and protocols—including classification of application subcategories that include voice, video, and IM. These are some examples of the types of apps and protocols BIG-IP PEM supports:

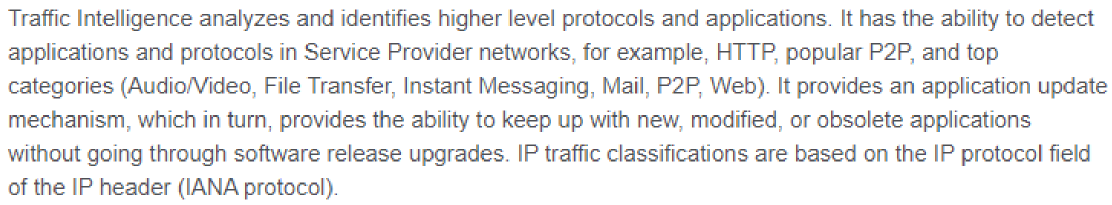
- P2P: BitTorrent, Gnutella
- VoIP: SIP, Skype, Yahoo!, Jabber
- Web: HTTP, HTTPS, FTP, YouTube, Facebook
- Streaming: HTTP streaming, RTSP, HTTP audio
- Non-TCP/UDP: IPsec, GRE, IPinIP, ICMP

Fig. 9

Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, last accessed May 14, 2020, Exhibit A

BIG-IP PEM includes predefined classification signatures for classifying traffic. The BIG-IP PEM collects traffic flows of the relevant user traffic and compares it to a set of known protocol signatures. See Fig. 10 & Fig. 11.

Citation 10: Classification signatures



Traffic Intelligence analyzes and identifies higher level protocols and applications. It has the ability to detect applications and protocols in Service Provider networks, for example, HTTP, popular P2P, and top categories (Audio/Video, File Transfer, Instant Messaging, Mail, P2P, Web). It provides an application update mechanism, which in turn, provides the ability to keep up with new, modified, or obsolete applications without going through software release upgrades. IP traffic classifications are based on the IP protocol field of the IP header (IANA protocol).

Fig. 10

Source: https://techdocs.f5.com/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-13-1-0/24.html, Page 1, Last accessed May 14, 2020, Exhibit E

Exhibit 2

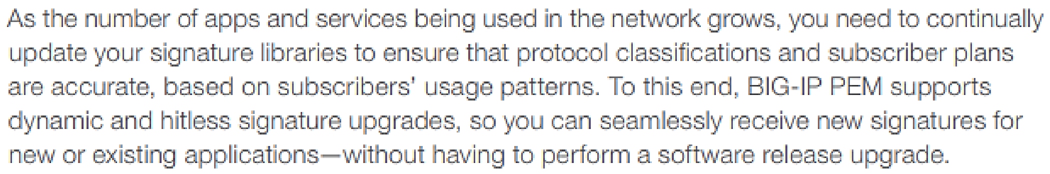
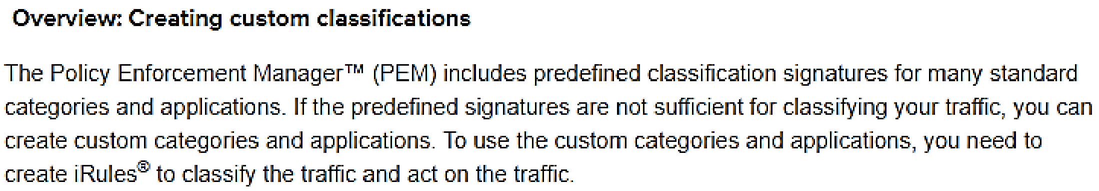
		Citation 11: Signature libraries  As the number of apps and services being used in the network grows, you need to continually update your signature libraries to ensure that protocol classifications and subscriber plans are accurate, based on subscribers' usage patterns. To this end, BIG-IP PEM supports dynamic and hitless signature upgrades, so you can seamlessly receive new signatures for new or existing applications—without having to perform a software release upgrade. **Fig. 11** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, Last accessed May 14, 2020, Exhibit A
15c. determining that a match exists between the collected traffic flows of the relevant user traffic and one or more members of the set known protocol signatures;	In step 420 a **determination is made whether a match exists between the collected traffic flows and any member of the set of known protocol signatures.** When a determination is made in step 420 that no match exists between the collected traffic flows and any member of the set of known protocol signa tures, the method 400 returns to step 410 where the collection of relevant	The method practiced by the accused product determines that a match exists between the collected traffic flows of the relevant user traffic and one or more members of the set known protocol signatures. BIG-IP PEM includes predefined classification signatures for classifying traffic. See Fig. 12 & Fig. 13. **Citation 12: Classification signatures**  **Overview: Creating custom classifications** The Policy Enforcement Manager™ (PEM) includes predefined classification signatures for many standard categories and applications. If the predefined signatures are not sufficient for classifying your traffic, you can create custom categories and applications. To use the custom categories and applications, you need to create iRules® to classify the traffic and act on the traffic. **Fig. 12** Source: https://techdocs.f5.com/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-11-6-0/18.html, Page 1, Last accessed May 14, 2020, Exhibit C **Citation 13: Signature libraries**

Exhibit 2

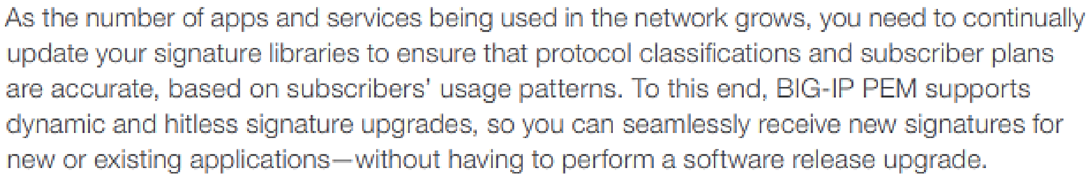
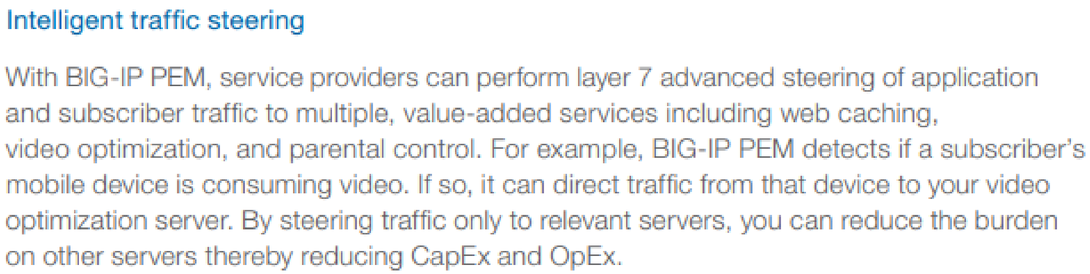
	user traffic continues. [Col. 11, Line 59-62]	 As the number of apps and services being used in the network grows, you need to continually update your signature libraries to ensure that protocol classifications and subscriber plans are accurate, based on subscribers' usage patterns. To this end, BIG-IP PEM supports dynamic and hitless signature upgrades, so you can seamlessly receive new signatures for new or existing applications—without having to perform a software release upgrade. **Fig. 13** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, Last accessed May 14, 2020, Exhibit A The BIG-IP PEM determines that a match exists between the collected traffic flows of the relevant user traffic and one or more members of the set known protocol signatures. For example, BIG-IP PEM detects that a subscriber's mobile device is consuming video, see Fig. 14 **Citation 14**  Intelligent traffic steering With BIG-IP PEM, service providers can perform layer 7 advanced steering of application and subscriber traffic to multiple, value-added services including web caching, video optimization, and parental control. For example, BIG-IP PEM detects if a subscriber's mobile device is consuming video. If so, it can direct traffic from that device to your video optimization server. By steering traffic only to relevant servers, you can reduce the burden on other servers thereby reducing CapEx and OpEx. **Fig. 14** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 3, last accessed May 14, 2020, Exhibit A
15d. identifying a flow sequence of video content information in the	PSI 340 **identifies the flow sequence of the video content**	The method practiced by the accused product identifies a flow sequence of video content information in the relevant user traffic.

Exhibit 2

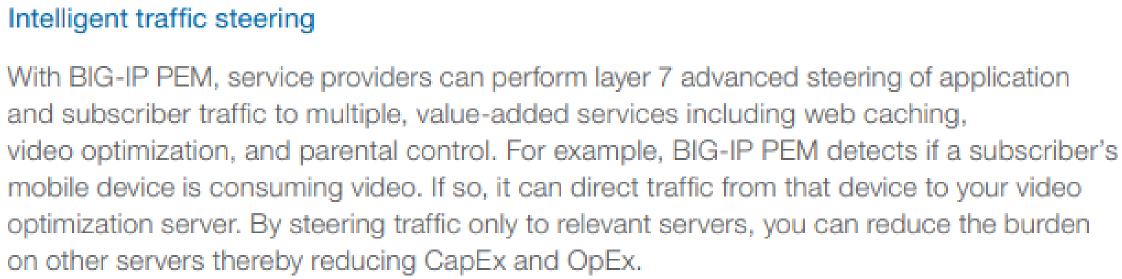
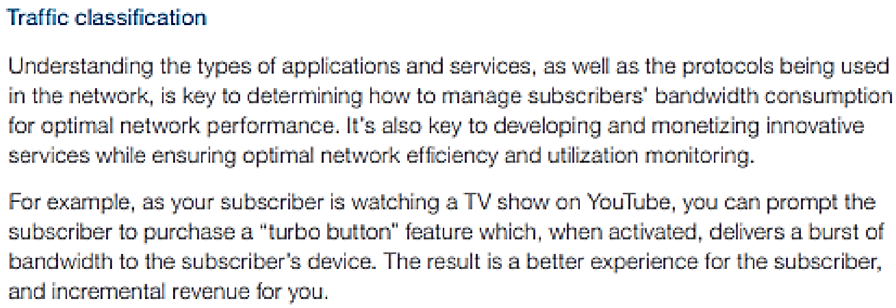
relevant user traffic;	**information** exchanged between VCA 307 and VSA 322 (or, more broadly, between terminal device 305 and VCS 320). Accordingly, PSI 340 identifies a protocol signature of the video content request 370 and of the video content delivery 395 to signify a particular video content flow. [Col. 9, Line 12-18]	The BIG-IP PEM classifies traffic using signature and identifies video content information in the relevant user traffic. For example, the BIG-IP PEM detects that a subscriber's mobile device is consuming video. see Fig. 15 and Fig. 16 **Citation 15: Traffic Steering**  Intelligent traffic steering With BIG-IP PEM, service providers can perform layer 7 advanced steering of application and subscriber traffic to multiple, value-added services including web caching, video optimization, and parental control. For example, BIG-IP PEM detects if a subscriber's mobile device is consuming video. If so, it can direct traffic from that device to your video optimization server. By steering traffic only to relevant servers, you can reduce the burden on other servers thereby reducing CapEx and OpEx. **Fig. 15** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 3, last accessed May 14, 2020, Exhibit A **Citation 16: Targeted content delivery**  Traffic classification Understanding the types of applications and services, as well as the protocols being used in the network, is key to determining how to manage subscribers' bandwidth consumption for optimal network performance. It's also key to developing and monetizing innovative services while ensuring optimal network efficiency and utilization monitoring. For example, as your subscriber is watching a TV show on YouTube, you can prompt the subscriber to purchase a "turbo button" feature which, when activated, delivers a burst of bandwidth to the subscriber's device. The result is a better experience for the subscriber, and incremental revenue for you. **Fig. 16** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf,

Exhibit 2

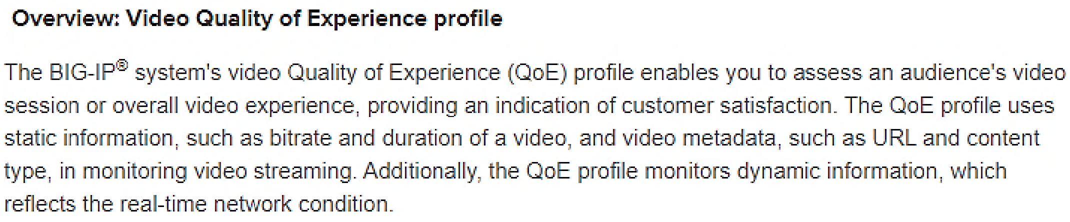
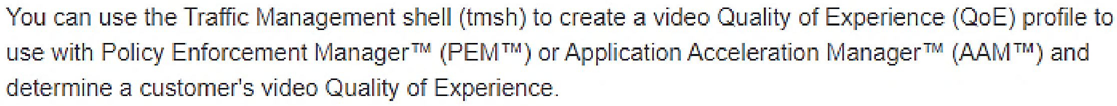
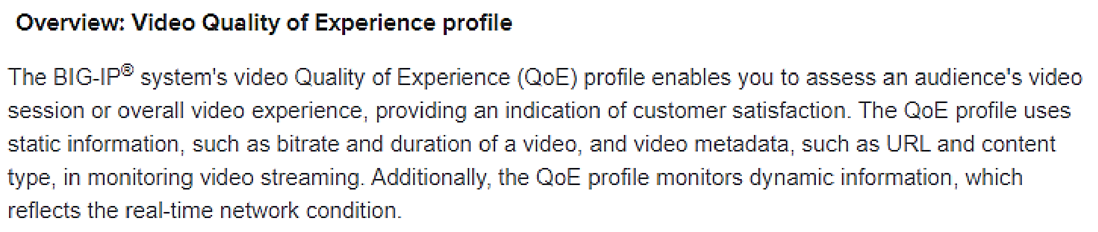
		Page 2, last accessed May 14, 2020, Exhibit A
15e. monitoring and analyzing the video content information;	the PSI 340 **monitors and extracts raw metadata text streams from metadata flow 375.** As discussed elsewhere herein, the raw metadata text streams monitored and extracted by PSI 340 are associated with the video content flow of video content delivery 395 from the online traffic. [Col. 9, Line 27-32]	The method practiced by the accused product monitors and analyzes the video content information. The BIG-IP system Quality of Experience (QoE) profile assesses an audience's video session. BIG-IP uses video's metadata such as URL and content type in monitoring streaming. The traffic sent to the QoE profile can be classified by deep packet inspection in BIG-IP PEM. A video QoE profile can be created to use with the BIG-IP PEM to determine a customer's video QoE. See Fig. 17 and Fig. 18. **Citation 17: Video Metadata**  **Overview: Video Quality of Experience profile** The BIG-IP® system's video Quality of Experience (QoE) profile enables you to assess an audience's video session or overall video experience, providing an indication of customer satisfaction. The QoE profile uses static information, such as bitrate and duration of a video, and video metadata, such as URL and content type, in monitoring video streaming. Additionally, the QoE profile monitors dynamic information, which reflects the real-time network condition. **Fig. 17** Source: https://techdocs.f5.com/kb/en-us/products/big-ip-aam/manuals/product/aam-implementations-11-6-0/18.html, Page 5, Last accessed May 14, 2020, Exhibit D **Citation 18: QoE profile to use with PEM**  You can use the Traffic Management shell (tmsh) to create a video Quality of Experience (QoE) profile to use with Policy Enforcement Manager™ (PEM™) or Application Acceleration Manager™ (AAM™) and determine a customer's video Quality of Experience. **Fig. 18** Source: https://techdocs.f5.com/kb/en-us/products/big-ip-aam/manuals/product/aam-

Exhibit 2

implementations-11-6-0/18.html, Page 7, Last accessed May 14, 2020, Exhibit D

The BIG-IP system Quality of Experience (QoE) profile assesses an audience's video session. The QoE profiles use static information such as the content type of a video in the monitored video stream viewed by a user. See Fig. 19.

Citation 19: Video Metadata



Overview: Video Quality of Experience profile

The BIG-IP® system's video Quality of Experience (QoE) profile enables you to assess an audience's video session or overall video experience, providing an indication of customer satisfaction. The QoE profile uses static information, such as bitrate and duration of a video, and video metadata, such as URL and content type, in monitoring video streaming. Additionally, the QoE profile monitors dynamic information, which reflects the real-time network condition.

Fig. 19

Source: https://techdocs.f5.com/kb/en-us/products/big-ip-aam/manuals/product/aam-implementations-11-6-0/18.html, Page 5, Last accessed May 14, 2020, Exhibit D

The BIG-IP PEM classifies traffic using signature and identifies video content information in the relevant user traffic (i.e. monitors and analyzes the video content information). For example, the BIG-IP PEM detects that a subscriber's mobile device is consuming video, see Fig. 20 & Fig. 21

Citation 20: Traffic steering

Exhibit 2

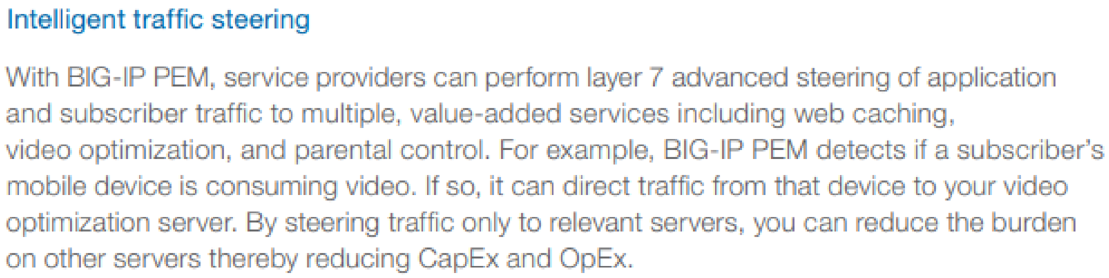
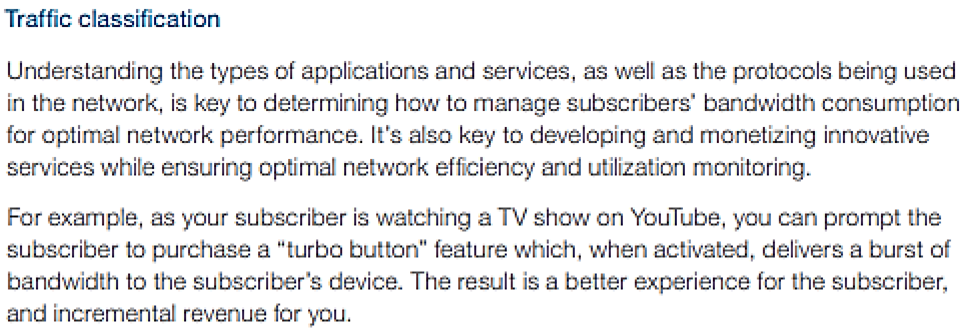
		 Intelligent traffic steering With BIG-IP PEM, service providers can perform layer 7 advanced steering of application and subscriber traffic to multiple, value-added services including web caching, video optimization, and parental control. For example, BIG-IP PEM detects if a subscriber's mobile device is consuming video. If so, it can direct traffic from that device to your video optimization server. By steering traffic only to relevant servers, you can reduce the burden on other servers thereby reducing CapEx and OpEx. **Fig. 20** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 3, last accessed May 14, 2020, Exhibit A **Citation 21: Targeted content delivery**  Traffic classification Understanding the types of applications and services, as well as the protocols being used in the network, is key to determining how to manage subscribers' bandwidth consumption for optimal network performance. It's also key to developing and monetizing innovative services while ensuring optimal network efficiency and utilization monitoring. For example, as your subscriber is watching a TV show on YouTube, you can prompt the subscriber to purchase a "turbo button" feature which, when activated, delivers a burst of bandwidth to the subscriber's device. The result is a better experience for the subscriber, and incremental revenue for you. **Fig. 21** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, last accessed May 14, 2020, Exhibit A
15f. using deep packet inspection (DPI) technology in a metadata information collector to	**Deep packet inspection (DPI) technology is deployed by carriers in current embodiments to**	The method practiced by the accused product uses deep packet inspection (DPI) technology in a metadata information collector to identify and extract metadata associated with the video content information in the packet-based communication network.

Exhibit 2

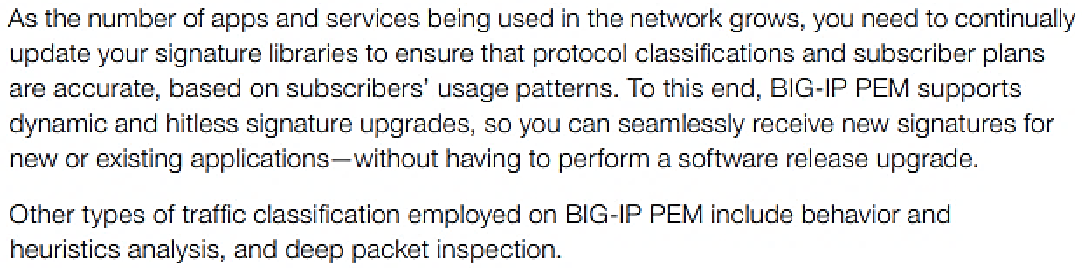
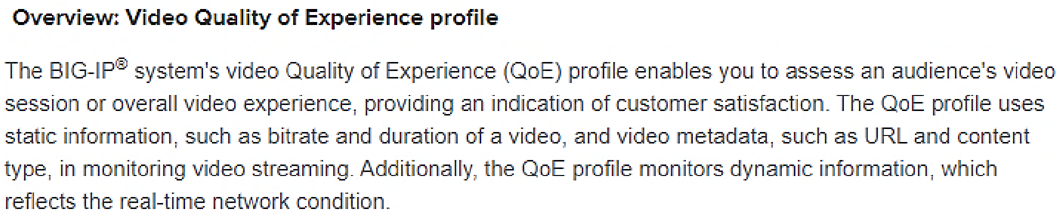
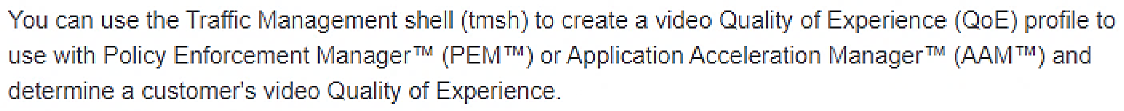
identify and extract metadata associated with the video content information in the packet-based communication network;	**monitor Internet traffic for the purposes of traffic control and engineering**. Some current embodiments utilize DPI for the purposes of targeted content delivery. [Col. 1, Line 42-46]	BIG-IP PEM uses deep packet inspection for traffic classification. See Fig. 22 **Citation 22: Deep packet inspection**  As the number of apps and services being used in the network grows, you need to continually update your signature libraries to ensure that protocol classifications and subscriber plans are accurate, based on subscribers' usage patterns. To this end, BIG-IP PEM supports dynamic and hitless signature upgrades, so you can seamlessly receive new signatures for new or existing applications—without having to perform a software release upgrade. Other types of traffic classification employed on BIG-IP PEM include behavior and heuristics analysis, and deep packet inspection. **Fig. 22** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, Last accessed May 14, 2020, Exhibit A The BIG-IP system Quality of Experience (QoE) profile assesses an audience's video session. BIG-IP uses video's metadata such as URL and content type in monitoring streaming. The traffic sent to the QoE profile can be classified by deep packet inspection in BIG-IP PEM. A video QoE profile can be created to use with the BIG-IP PEM to determine a customer's video QoE. See Fig. 23 and Fig. 24 **Citation 23: Video Metadata**  **Overview: Video Quality of Experience profile** The BIG-IP® system's video Quality of Experience (QoE) profile enables you to assess an audience's video session or overall video experience, providing an indication of customer satisfaction. The QoE profile uses static information, such as bitrate and duration of a video, and video metadata, such as URL and content type, in monitoring video streaming. Additionally, the QoE profile monitors dynamic information, which reflects the real-time network condition.

Exhibit 2

Fig. 23

Source: https://techdocs.f5.com/kb/en-us/products/big-ip-aam/manuals/product/aam-implementations-11-6-0/18.html, Page 5, Last accessed May 14, 2020, Exhibit D

Citation 24: QoE profile to use with PEM



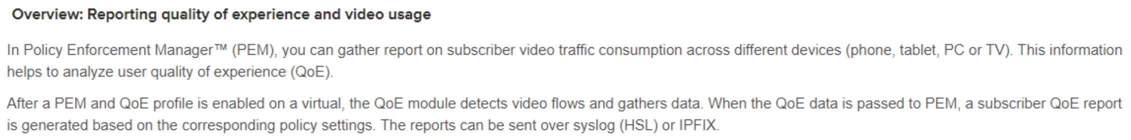
You can use the Traffic Management shell (tmsh) to create a video Quality of Experience (QoE) profile to use with Policy Enforcement Manager™ (PEM™) or Application Acceleration Manager™ (AAM™) and determine a customer's video Quality of Experience.

Fig. 24

Source: https://techdocs.f5.com/kb/en-us/products/big-ip-aam/manuals/product/aam-implementations-11-6-0/18.html, Page 7, Last accessed May 14, 2020, Exhibit D

BIG-IP PEM allows gathering reports on subscriber video traffic consumption. This information helps to analyze a user's QoE. When a QoE profile is enabled on a virtual server, the QoE module detects video flows and gathers data. A subscriber QoE report can be generated based on the policy settings when this data is passed to the PEM. See Fig. 25.

Citation 25: QoE reporting in BIG-IP PEM



Overview: Reporting quality of experience and video usage

In Policy Enforcement Manager™ (PEM), you can gather report on subscriber video traffic consumption across different devices (phone, tablet, PC or TV). This information helps to analyze user quality of experience (QoE).

After a PEM and QoE profile is enabled on a virtual, the QoE module detects video flows and gathers data. When the QoE data is passed to PEM, a subscriber QoE report is generated based on the corresponding policy settings. The reports can be sent over syslog (HSL) or IPFIX.

Fig. 25

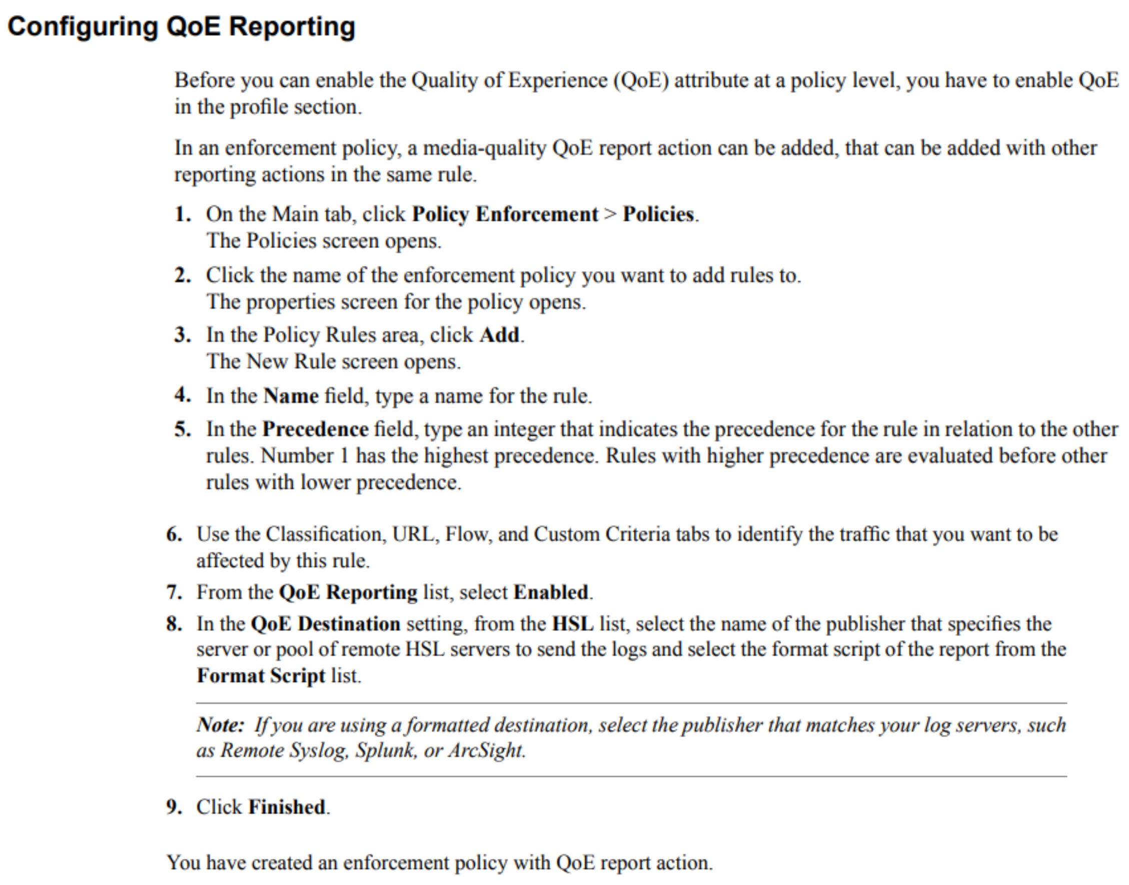
Source: https://techdocs.f5.com/content/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-12-1-0/_jcr_content/pdfAttach/download/file.res/BIG-IP_Policy_Enforcement_Manager__Implementations.pdf, Page 59, Last Accessed September 2,

Exhibit 2

2020, Exhibit F

BIG-IP PEM allows configuring of the enforcement policies. In an enforcement policy, a media-quality QoE report action can be added. See Fig. 26.

Citation 26: Enforcement policy with QoE report action



Configuring QoE Reporting

Before you can enable the Quality of Experience (QoE) attribute at a policy level, you have to enable QoE in the profile section.

In an enforcement policy, a media-quality QoE report action can be added, that can be added with other reporting actions in the same rule.

1. On the Main tab, click **Policy Enforcement** > **Policies**.
   The Policies screen opens.
2. Click the name of the enforcement policy you want to add rules to.
   The properties screen for the policy opens.
3. In the Policy Rules area, click **Add**.
   The New Rule screen opens.
4. In the **Name** field, type a name for the rule.
5. In the **Precedence** field, type an integer that indicates the precedence for the rule in relation to the other rules. Number 1 has the highest precedence. Rules with higher precedence are evaluated before other rules with lower precedence.
6. Use the Classification, URL, Flow, and Custom Criteria tabs to identify the traffic that you want to be affected by this rule.
7. From the **QoE Reporting** list, select **Enabled**.
8. In the **QoE Destination** setting, from the **HSL** list, select the name of the publisher that specifies the server or pool of remote HSL servers to send the logs and select the format script of the report from the **Format Script** list.

   Note: *If you are using a formatted destination, select the publisher that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*
9. Click **Finished**.

You have created an enforcement policy with QoE report action.

Fig. 26

Source: https://techdocs.f5.com/content/kb/en-us/products/big-ip-pem/manuals/product/pem-

Exhibit 2

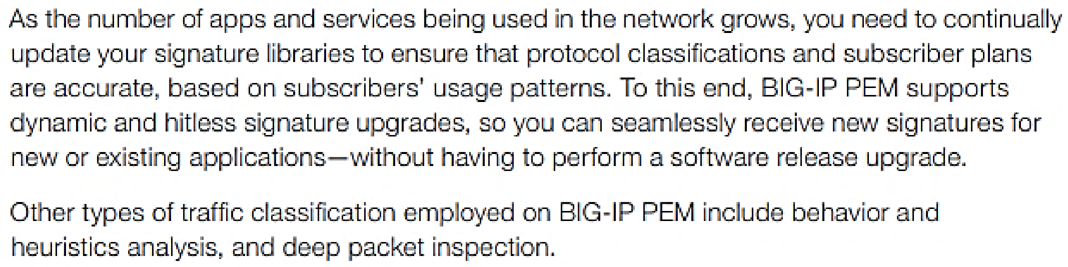
		implementations-12-1-0/_jcr_content/pdfAttach/download/file.res/BIG-IP_Policy_Enforcement_Manager__Implementations.pdf, Page 60-61, Last Accessed September 2, 2020, Exhibit F
15g. forwarding the extracted metadata; **15h.** harmonizing the forwarded metadata into a common format, wherein the common format is a hierarchy of class structure;	In various exemplary embodiments, **the MPP 350 harmonizes or unifies various forms of metadata into a common format**, including performing a formatting conversion if necessary. **In various exemplary embodiments, the harmonized or unified formatted metadata is then conveyed to behavior analyzer 330.** [Col. 10, Line 21-26] In various exemplary embodiments, **the common format given to metadata by MPP 350 for transmission to behavior analyzer 330 is**	The method practiced by the accused product forwards the extracted metadata and harmonizing the forwarded metadata into a common format, wherein the common format is a hierarchy of class structure. BIG-IP PEM uses deep packet inspection for traffic classification. See Fig. 27 **Citation 27: Deep packet inspection**  As the number of apps and services being used in the network grows, you need to continually update your signature libraries to ensure that protocol classifications and subscriber plans are accurate, based on subscribers' usage patterns. To this end, BIG-IP PEM supports dynamic and hitless signature upgrades, so you can seamlessly receive new signatures for new or existing applications—without having to perform a software release upgrade. Other types of traffic classification employed on BIG-IP PEM include behavior and heuristics analysis, and deep packet inspection. **Fig. 27** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, Last accessed May 14, 2020, Exhibit A BIG-IP PEM classifies traffic into several categories of applications and protocols such as classification of application subcategories that include voice, video, and IM. See Fig. 28. **Citation 28: Traffic classification**

Exhibit 2

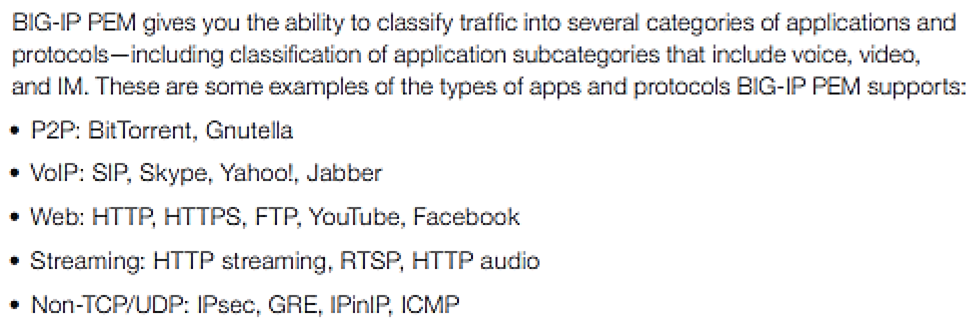
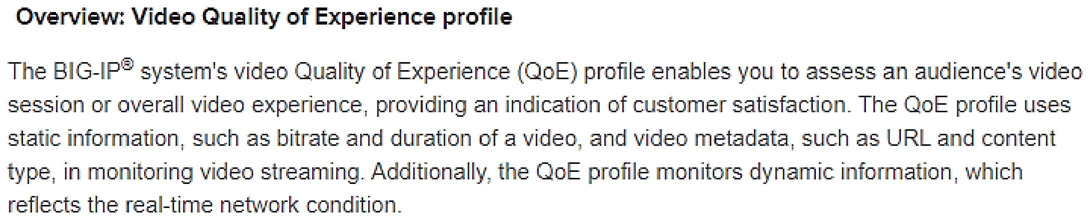
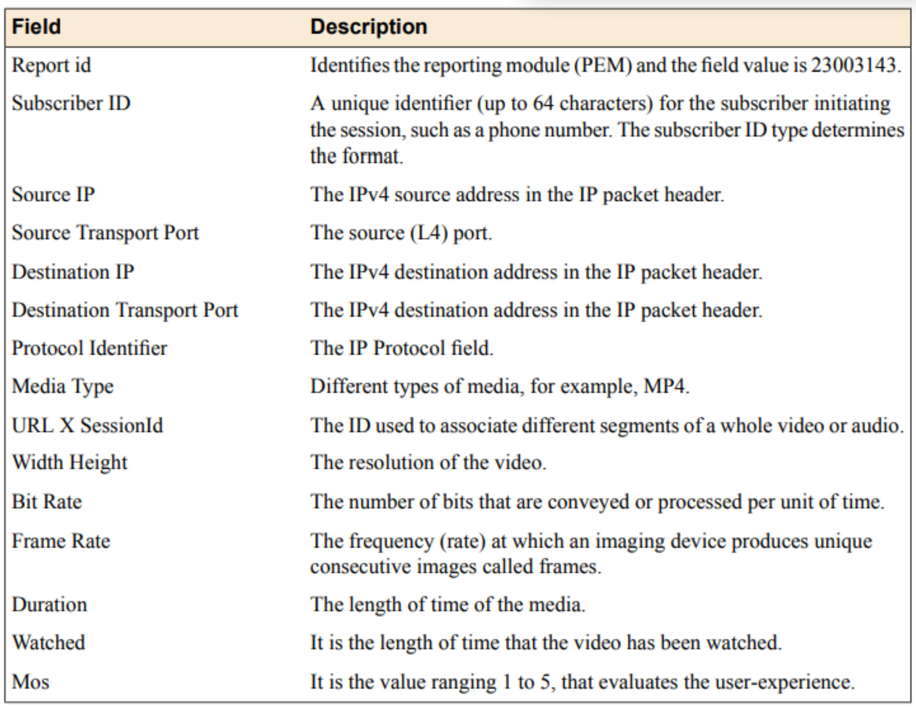
	defined as a form of schema or a hierarchy of class structure. Examples of a form of schema include those containing a year, a genre, a rating, a production house, a lead actor, a lead actress, a Suitable audience, and so on. [Col. 10, Line 29-34]	 BIG-IP PEM gives you the ability to classify traffic into several categories of applications and protocols—including classification of application subcategories that include voice, video, and IM. These are some examples of the types of apps and protocols BIG-IP PEM supports: • P2P: BitTorrent, Gnutella • VoIP: SIP, Skype, Yahoo!, Jabber • Web: HTTP, HTTPS, FTP, YouTube, Facebook • Streaming: HTTP streaming, RTSP, HTTP audio • Non-TCP/UDP: IPsec, GRE, IPinIP, ICMP **Fig. 28** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, last accessed May 14, 2020, Exhibit A The BIG-IP system Quality of Experience (QoE) profile assesses an audience's video session. BIG-IP uses video's metadata such as URL and content type in monitoring streaming. See Fig. 29. Thus, based on the traffic classification, BIG-IP PEM stores the metadata of the videos. **Citation 29: Video Metadata**  **Overview: Video Quality of Experience profile** The BIG-IP® system's video Quality of Experience (QoE) profile enables you to assess an audience's video session or overall video experience, providing an indication of customer satisfaction. The QoE profile uses static information, such as bitrate and duration of a video, and video metadata, such as URL and content type, in monitoring video streaming. Additionally, the QoE profile monitors dynamic information, which reflects the real-time network condition. **Fig. 29** Source: https://techdocs.f5.com/kb/en-us/products/big-ip-aam/manuals/product/aam-implementations-11-6-0/18.html, Page 5, Last accessed May 14, 2020, Exhibit D

Exhibit 2

In BIG-IP PEM, an enforcement policy can send QoE-based information (i.e. metadata) about traffic that matches certain criteria to an external high-speed logging server. A QoE-based report (i.e. common format) is generated comprising the metadata includes static information such as bitrate and duration of the video, and also dynamic information such as Mean Opinion Score (MOS) which reflects the real-time network condition i.e. (a schema to store different metadata values). See Fig. 30.

Citation 30: QoE-based reporting format

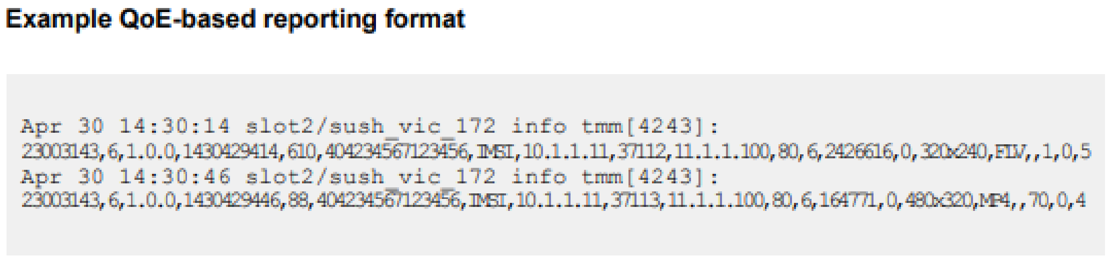


Field	Description
Report id	Identifies the reporting module (PEM) and the field value is 23003143.
Subscriber ID	A unique identifier (up to 64 characters) for the subscriber initiating the session, such as a phone number. The subscriber ID type determines the format.
Source IP	The IPv4 source address in the IP packet header.
Source Transport Port	The source (L4) port.
Destination IP	The IPv4 destination address in the IP packet header.
Destination Transport Port	The IPv4 destination address in the IP packet header.
Protocol Identifier	The IP Protocol field.
Media Type	Different types of media, for example, MP4.
URL X SessionId	The ID used to associate different segments of a whole video or audio.
Width Height	The resolution of the video.
Bit Rate	The number of bits that are conveyed or processed per unit of time.
Frame Rate	The frequency (rate) at which an imaging device produces unique consecutive images called frames.
Duration	The length of time of the media.
Watched	It is the length of time that the video has been watched.
Mos	It is the value ranging 1 to 5, that evaluates the user-experience.

Fig. 30

Source: https://techdocs.f5.com/content/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-12-1-0/_jcr_content/pdfAttach/download/file.res/BIG-

Exhibit 2

		IP_Policy_Enforcement_Manager__Implementations.pdf, Page 61, Last Accessed September 2, 2020, Exhibit F
		An example QoE-based report is seen in Fig. 31.
		Citation 31: Example QoE-based reporting format
		
		Example QoE-based reporting format
		`Apr 30 14:30:14 slot2/sush_vic_172 info tmm[4243]:`
		`23003143,6,1.0.0,1430429414,610,404234567123456,IMSI,10.1.1.11,37112,11.1.1.100,80,6,2426616,0,320x240,FLV,,1,0,5`
		`Apr 30 14:30:46 slot2/sush_vic_172 info tmm[4243]:`
		`23003143,6,1.0.0,1430429446,88,404234567123456,IMSI,10.1.1.11,37113,11.1.1.100,80,6,164771,0,480x320,MP4,,70,0,4`
		Fig. 31
		Source: https://techdocs.f5.com/content/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-12-1-0/_jcr_content/pdfAttach/download/file.res/BIG-IP_Policy_Enforcement_Manager__Implementations.pdf, Page 62, Last Accessed September 2, 2020, Exhibit F
		Note: Source code review could further help in gathering additional evidence related to the claim limitation "*harmonizing the forwarded metadata into a common format, wherein the common format is a hierarchy of class structure*"

15i. developing a user profile based on the harmonized metadata; and	In various exemplary embodiments, such **content related metadata information is**	The method practiced by the accused product develops a user profile based on the harmonized metadata and delivering targeted content based on the developed user profile. With the BIG-IP PEM video analytics capability, service providers can get enhanced visibility

Exhibit 2

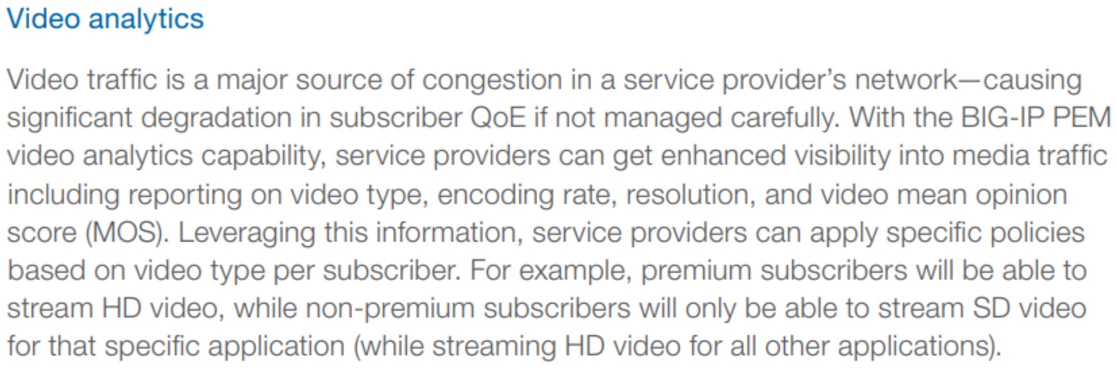
15j. delivering targeted content based on the developed user profile.	**further utilized by the behavior analyzer 330 to infer the user profile.** Accordingly, this information is relevant in various exemplary embodiments to forming a demographic and psychographic portion of the user profile. In various exemplary embodiments, **the targeted content delivery infrastructure 335 utilizes the established user profile data and delivers highly relevant and personalized content to end users of the terminal device 305.** [Col. 11, Line 18-26]	into media traffic including reporting on video type, encoding rate, resolution, and video mean opinion score (MOS). Leveraging this information, specific policies can be applied based on video type per subscriber (i.e. a user profile is developed based on the metadata). These policies can be configured to deliver targeted content for the user. See Fig. 32. **Citation 32: Video analytics**  Video analytics Video traffic is a major source of congestion in a service provider's network—causing significant degradation in subscriber QoE if not managed carefully. With the BIG-IP PEM video analytics capability, service providers can get enhanced visibility into media traffic including reporting on video type, encoding rate, resolution, and video mean opinion score (MOS). Leveraging this information, service providers can apply specific policies based on video type per subscriber. For example, premium subscribers will be able to stream HD video, while non-premium subscribers will only be able to stream SD video for that specific application (while streaming HD video for all other applications). **Fig. 32** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 3, last accessed May 14, 2020, Exhibit A The BIG IP system including the BIG-IP PEM enables the service providers to insert content (i.e. targeted content delivery) to offer personalized services to benefit subscribers (i.e. based on their user profiles). BIG-IP PEM helps in gaining subscriber and context awareness (PEM uses subscriber awareness along with the metadata to develop user profile), and a deep understanding of subscribers' mobile preferences. See Fig. 33 & Fig. 34. **Citation 33: Content Insertion**

Exhibit 2

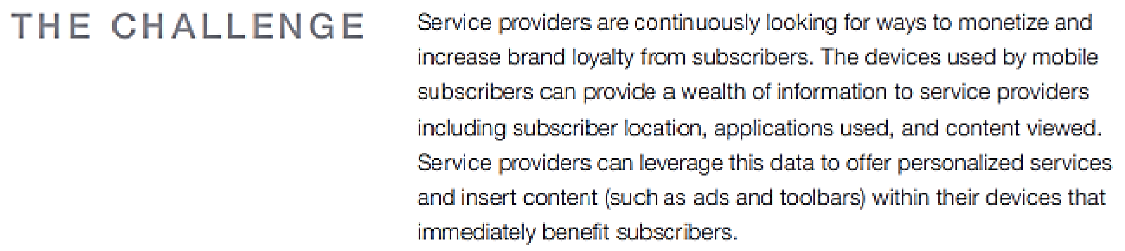
		 THE CHALLENGE Service providers are continuously looking for ways to monetize and increase brand loyalty from subscribers. The devices used by mobile subscribers can provide a wealth of information to service providers including subscriber location, applications used, and content viewed. Service providers can leverage this data to offer personalized services and insert content (such as ads and toolbars) within their devices that immediately benefit subscribers. **Fig. 33** Source: https://f5.com/Portals/1/Premium/Architectures/GUIDE-SP-CCNF-66589956-customer-usecase-2016-spreads.pdf, Page 17, Last accessed May 14, 2020, Exhibit B **Citation 34: Content Insertion**

Exhibit 2

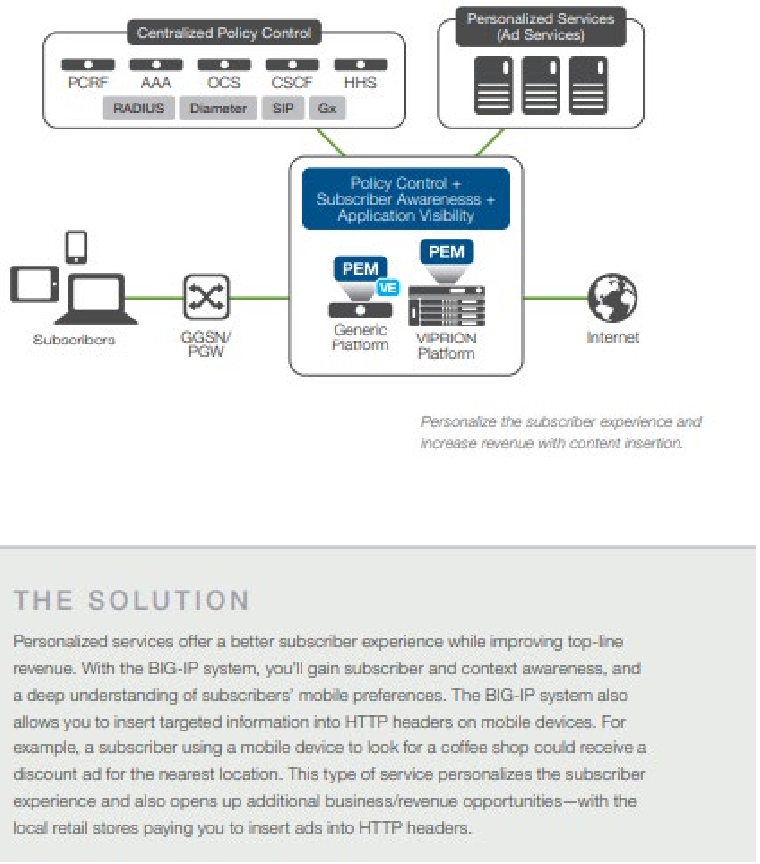
		 Centralized Policy Control PCRF AAA OCS CSCF HHS RADIUS Diameter SIP Gx Personalized Services (Ad Services) Policy Control + Subscriber Awareness + Application Visibility PEM VE PEM Subscribers GGSN/ PGW Generic Platform VIPRION Platform Internet *Personalize the subscriber experience and increase revenue with content insertion.* THE SOLUTION Personalized services offer a better subscriber experience while improving top-line revenue. With the BIG-IP system, you'll gain subscriber and context awareness, and a deep understanding of subscribers' mobile preferences. The BIG-IP system also allows you to insert targeted information into HTTP headers on mobile devices. For example, a subscriber using a mobile device to look for a coffee shop could receive a discount ad for the nearest location. This type of service personalizes the subscriber experience and also opens up additional business/revenue opportunities—with the local retail stores paying you to insert ads into HTTP headers. **Fig. 34** Source: https://f5.com/Portals/1/Premium/Architectures/GUIDE-SP-CCNF-66589956-customer-usecase-2016-spreads.pdf, Page 17, Last accessed May 14, 2020, Exhibit B Similarly, the BIG-IP PEM detects if a subscriber's device is consuming video such as using viewing any TV show on YouTube (i.e. consuming video traffic). Then based on the user's profile, the BIG-IP PEM delivers targeted content such as shown in Fig. 35 and Fig. 36.

Exhibit 2

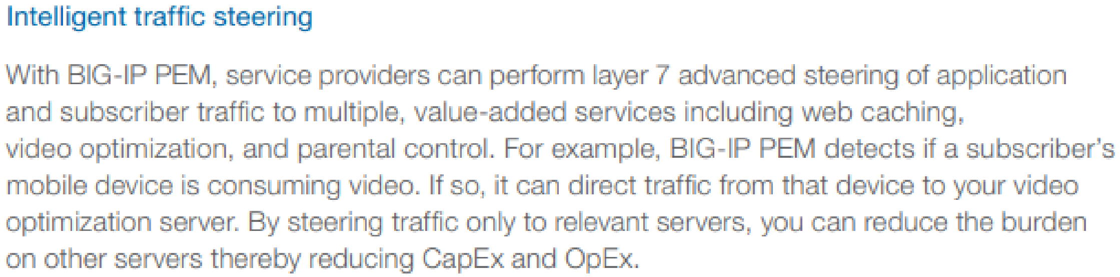
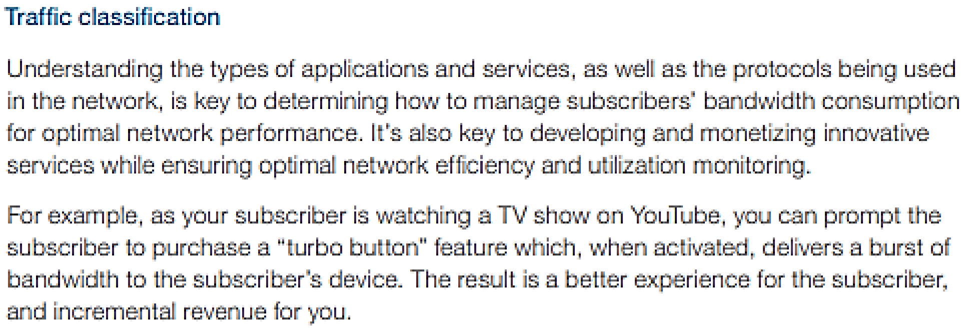
		Citation 35: Traffic steering  Intelligent traffic steering With BIG-IP PEM, service providers can perform layer 7 advanced steering of application and subscriber traffic to multiple, value-added services including web caching, video optimization, and parental control. For example, BIG-IP PEM detects if a subscriber's mobile device is consuming video. If so, it can direct traffic from that device to your video optimization server. By steering traffic only to relevant servers, you can reduce the burden on other servers thereby reducing CapEx and OpEx. **Fig. 35** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 3, last accessed May 14, 2020, Exhibit A **Citation 36: Targeted content delivery**  Traffic classification Understanding the types of applications and services, as well as the protocols being used in the network, is key to determining how to manage subscribers' bandwidth consumption for optimal network performance. It's also key to developing and monetizing innovative services while ensuring optimal network efficiency and utilization monitoring. For example, as your subscriber is watching a TV show on YouTube, you can prompt the subscriber to purchase a "turbo button" feature which, when activated, delivers a burst of bandwidth to the subscriber's device. The result is a better experience for the subscriber, and incremental revenue for you. **Fig. 36** Source: https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf, Page 2, last accessed May 14, 2020, Exhibit A

Exhibit 2

References Cited

Exhibit(s)	**Description**	**Link**
Exhibit A	BIG-IP Policy Enforcement Manager (PEM) - Datasheet	https://www.f5.com/pdf/products/big-ip-policy-enforcement-manager-datasheet.pdf
Exhibit B	F5 Handbook for Service Providers	https://f5.com/Portals/1/Premium/Architectures/GUIDE-SP-CCNF-66589956-customer-usecase-2016-spreads.pdf
Exhibit C	BIG-IP PEM Classification signatures	https://techdocs.f5.com/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-11-6-0/18.html
Exhibit D	BIG-IP Video delivery Optimization	https://techdocs.f5.com/kb/en-us/products/big-ip-aam/manuals/product/aam-implementations-11-6-0/18.html
Exhibit E	BIG-IP Custom Classifications	https://techdocs.f5.com/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-13-1-0/24.html
Exhibit F	BIG-IP PEM Implementations	https://techdocs.f5.com/content/kb/en-us/products/big-ip-pem/manuals/product/pem-implementations-12-1-0/_jcr_content/pdfAttach/download/file.res/BIG-IP_Policy_Enforcement_Manager__Implementations.pdf